**ATTACHMENT 3 SYSTEM B - TRAUMA REGISTRY TECHNICAL REQUIREMENTS**

The following requirements describe what is needed to support DHHS technical project operations. Please provide a response to each of the below requirements. Any deviations to the requirements for the system must be noted in Attachment 1 and attached as a separate document. There are two parts of Attachment 1 for each system:

1. Deviations to Section (V)(A), (V)(B), (V)(D), and (V)(E).
2. Deviations to Section (V)(C).

Architecture Requirements

| **Req #** | **Requirement** |
| --- | --- |
| ARCH-1 | The bidder must provide the following architectural details about their solution.  **Technology Architecture:** This describes the software components, including third-party software products, open-source libraries, and utilities that complete platform for running a service or supporting an application. This section should document any technical requirements for accessing the software, including but not limited to client desktop installs, etc. Further, the section should clearly outline any State required infrastructure, such as setting up VPN, SFTP, etc., to implement or operate the system.  **Network Architecture**: This describes the means of communication, the method of sending and receiving information, between the assets in the Technology Architecture.  **Application Architecture**: This describes how the solution components are assembled and interact to meet the business needs. The application architecture should address the following.   * How the proposed application architecture is responsive to mobile technology and works with mobile devices such as smartphones or tablets. * If needed, how the solution manages and stores documents and attachments. Please provide details of the architecture’s ability to integrate with enterprise document management systems.   **Data Flow Architecture**: This should provide a written description of the data flows that articulate and clearly identify anywhere State data is to be processed, stored, or transmitted.  • clearly delineate how data comes into and out of the system boundary.  • clearly identify data flows for privileged, non-privileged, and customer access; and  • depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.  **Scalability and High Availability Architecture**: This should describe and address the following:  • How the system architecture supports scaling with increased load  • How the system provides high availability to support minimum disruptions to the business operations  • How the solution handles notifications when a component or interface endpoint is unavailable.  • Proposed system performance functionality and monitoring tools.  • How the solution handles recovery of failed transactions because of a component failure.  • How the solution is available online 24 hours a day and 7 days a week, 99.5% of the time each month |
| Response: | | |
| ARCH-2 | The bidder must describe the nature of their software application and address the following.  • Type of Software – SaaS or On-Premises or Hosted Application software  • Licensing Model- Perpetual or Subscription based licenses.  • Single or Multi-Tenant architecture |
| Response: | | |
| ARCH-3 | The Bidder must propose a cloud-based hosting environment for the solution and all module components.  Describe any independent third-party certifications and other independent third-party security assessments available for the proposed cloud environment and module components including the frequency of renewal of the certifications or assessments.  Assessment examples include SSAE SOC 2 Type 2, FedRAMP Certification, or a NIST 800-53 rev 5 moderate assessment.  Please note that it is a State of Nebraska requirement that all data associated with the solution or its components must reside within the United States. |
| Response: | | |
| ARCH-4 | The Bidder must describe it approach to support multiple environments concurrently to support the following.   * Provide sufficient environments and configurations necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery). * Implementing and using de-identified data in non-production environments. |
| Response: | | |
| ARCH-5 | The Bidder's proposed solution must comply with accessibility requirements described in 45 CFR 85 and with State of Nebraska accessibility requirements located at http://www.nitc.nebraska.gov/standards/index. Html. The application/solution user interface must meet the Section 508 Compliance Standards. (https://www.section508.gov/manage/laws-and-policies/) |
| Response: | | |

**Security and Policy Compliance**

| **Req #** | **Requirement** |
| --- | --- |
| SPC-1 | The Bidder proposed solution must meet State and Federal IT standards and policies:  Describe how the proposed solution will conform to standards and policies such as:   * DHHS Information Technology {IT} Security Policies and Standards ( <https://dhhs.ne.gov/Documents/Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf#search=it%20security%20policy>) * Nebraska Information Technology Commission (NITC) Standards and Guidelines { <https://nitc.nebraska.gov/standards/index.html>) * Health Insurance Portability and Accountability Act (HIPAA) of 1996 * Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 * Nebraska Electronic Signature Statute [http://www.nebraskalegislature.gov/laws/statutes.php?statute=86-611](https://gcc02.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.nebraskalegislature.gov%2Flaws%2Fstatutes.php%3Fstatute%3D86-611&data=05%7C01%7CJennifer.Heck%40nebraska.gov%7Caf21f826e4e649f9ac5608db93584352%7C043207dfe6894bf6902001038f11f0b1%7C0%7C0%7C638265780750027122%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=7QkFZXRvtkJ8vH1Pbku%2BbgyjzAfc%2BzMnw611Gi1mtvE%3D&reserved=0) * Privacy Act of 1974 |
| Response: | | |
| SPC-2 | The Bidder must provide the Department with an annual independent third-party assessment of the security controls of the bidder and the proposed solution.  Describe the independent third-party certifications and other independent third-party security assessments available including the frequency of renewal of the certifications or assessments.  Assessment examples include SSAE SOC 2 Type 2 or a NIST 800-53 rev 5 moderate assessment.  Assessments should include level of risk for any identified security control gaps. |
| Response: | | |
| SPC-3 | The Bidder must conduct an annual independent third-party penetration test of the proposed solution and provide the results of the assessment to the Department.  Assessments should include testing for the OWASP Top 10 and include level of risk for any identified security findings.  Describe how the bidder will meet this requirement including providing an independent third-party penetration test prior to system go-live. |
| Response: | | |
| SPC-4 | The Bidder must describe its authentication framework of the proposed solution including the following:  • Authentication Standards  • Password Policy, including support for self-service password activities.  • End users’ ability to reset lost or expired passwords,  • Automatic log-off procedures  • Automatic account disablement after an Agency defined period of inactivity  • Administrators’ ability to lockout user(s).  • Support and approach for single sign-on  • Support and approach for how Multi-Factor Authentication  • Approach to handling failed logon attempts |
| Response: | | |
| SPC-5 | The Bidder must describe the authorization and account management framework of the proposed solution including the following:  •             Describe how the system uses role-based security and how users are assigned to roles.  •             Describe how user accounts are assigned and managed.  •             Describe available reports, such as a usage report listing all users and their last usage date.  •             Describe how the system supports authorization at an attribute/field level (edit, view etc.). |
| Response: | | |
| SPC-6 | The Bidder must describe the System Auditing functions of the solution including the following:  •             Describe in detail the data elements that are audited.  •             Describe the level of audit tracking being maintained.  •             Describe available audit reports.  •             Describe any automated audit log evaluation capabilities to identify security issues.  •             Describe how the proposed solution meets the Agency IT Auditing Standard (DHHS-IT-001F) found in DHHS Information Technology {IT} Security Policies and Standards ( <https://dhhs.ne.gov/Documents/Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf#search=it%20security%20policy>)  •             Describe how the bidder monitors, identifies, and reports on events impacting the system, such as attacks and other unauthorized use of the system. |
| Response: | | |

**Data Management Requirements**

| **Req #** | **Requirement** |
| --- | --- |
| DM-1 | The Bidder must describe how the solution handles and manages the data and how it separated from other tenants, ideally by providing a dedicated database or dedicated schema. |
| Response: | |
| DM-2 | The Bidder must encrypt data at rest and in transit. The bidder must describe its approach and use of industry standard cryptographic modules such as FIPS 140-2/-3 for encrypting data. |
| Response: | |
| DM-3 | The Bidder must provide the details of its approach and architecture to support the following.  • Data Handling when application and data is accessed via mobile device.   * Solution data synchronization if the solution supports off-line mode use. |
| Response: | |
| DM-4 | The Bidder must describe its integration design and approach and address the following.   * Ability to import data securely in industry standard formats (such as XML, JSON, CSV) in real-time and batch to support data intake from other State systems. * Ability to export data securely to industry standard formats (such as XML, JSON, CSV) to support data upload into the State Data Warehouse tools and systems, including platforms like Snowflake and Tableau, where appropriate. * Support for integration using industry standards approaches and principles such as REST APIs, Webservices etc. * Support for industry integration data standards such as Health level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR), X-12, HIPAA. * Provide documentation to support testing and collaboration with integrating systems. * Provide necessary documentation of the system's data dictionary which includes user-defined fields and tables. |
| Response: | |
| DM-5 | The Bidder must securely dispose of State data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 and must provide to the State a certificate of data destruction. |
| Response: | |
| DM-6 | The Bidder must describe its approach to Conversion and Migration Plan and address the following:  • Approach to conversion, cleansing, and migration.  • Approach to risk management for data conversion effort.  • Approach for testing the migration or the conversion of data.  • Approach to reporting the number of records successfully converted vs. errors or exceptions.  • Approach to resolving data conversion errors and issues.  • Approach for supporting the Department validation of converted data. |
| Response: | |
| DM-7 | The Bidder must meet the data retention requirements cited in 45 CFR 164.316 and the State's Administrative Rules.  Please describe your approach for their data retention. |
| Response: | |

**Operations Management**

| **Req #** | **Requirement** |
| --- | --- |
| OM-1 | The Bidder must outline their Business Continuity and Disaster Recovery (BCDR) approach that address the following.   * A BCDR Plan must be signed and approved by the State before any State data is transferred or entered the solution. The Plan must contain procedures for data backup, restoration, and emergency mode operations in the event of a. Hardware or Software Failures; b. Human Error; c. Natural Disaster; and/or d. Other unforeseeable emergencies. * Execute and successfully complete a full disaster recovery test before Go-Live. * Annually execute a full disaster recovery test and submit the results to the State. * Compliance with the Recovery Time Objective (RTO) of within 24 hours when the system outage is declared as a disaster. * Compliance with the Recovery Point Objective (RPO) of 2 hours of data lost before the disaster event. * Communication and Notification methodology to notify the relevant set of stakeholders. |
| Response: | |
| OM-2 | The bidder must describe its approach for all testing activities and address the following:   * Overall testing strategy and support for the following testing types: unit testing, system testing, integration testing, regression testing, user acceptance testing (UAT), parallel testing, performance, and load testing, manual and automated and/or scripted testing, and end-to-end integration testing of COTS products if any. * Approach to planning and preparing the test/staging environment. * Approach to conducting each test level. * Approach for testing nonfunctional requirements (security, performance, etc.) * Approach to test documentation (e.g., test cases, test scripts, test case matrices added as the design configuration progresses). * Approach to quality control/quality assurance. * Approach to test results reporting, traceability, and metrics. |
| Response: | |
| OM-3 | The bidder must describe their software maintenance process and address the following.  • Approach to managing software versions to ensure bidder support.  • Approach to Change Management, including defects and enhancements.  • Approach to testing and release management.  • Approach to maintaining integrations with external and internal trading partners. |
| Response: | |
| OM-4 | The bidder must describe their incident management process that will be used to report business and security incidents (such as any unauthorized access to or incidents where data may have been compromised). Please outline your incident notification time frames and how it complies with the State DHHS Information Technology {IT} Security Policies and Standards. |
| Response: | |
| OM-5 | The bidder must describe its approach on providing technical documentation that addresses the following.  • System Operation Manual  • Administrative Operations |
| Response: | |
| OM-6 | The bidder must describe its approach to use and integrate with the state JIRA infrastructure for user acceptance testing and, ongoing release testing. |
| Response: | |